



TITLE:

Supersingular Abelian Varietiesの算術的理論(Einstein計量とYang-Mills接続)

AUTHOR(S):

伊吹山, 知義

CITATION:

伊吹山, 知義. Supersingular Abelian Varietiesの算術的理論(Einstein計量とYang-Mills接続). 数理解析研究所講究録 1992, 775: 154-166

ISSUE DATE:

1992-03

URL:

<http://hdl.handle.net/2433/82423>

RIGHT:

Supersingular Abelian Varieties の算術的理論

大阪大学教養部 伊吹山 知義 (Tomoyoshi Ibukiyama)

§0. 序

幾何学的不変量が数論的不変量に関係していることは、よくあることである。特に Néron Severi 群が非常に大きい時などは、数論的概念の占める割合が大きいように思われる。

Supersingular elliptic curve の理論は、その一例で、Deuring 等により、数論との対応が非常によくわかっている。これがどの程度 Supersingular Abelian Varieties に一般化されるかを述べるのが、本稿の目的である。内容的には、多少桂利行氏 of 原稿と重複が生じるかもしれないが、その実は御容赦願いたい。また、誰による結果かは、その都度、明示することにしたい。

§1. 整数論的手法の例.

本稿の主テーマにはいる前に、簡単な例をあげて、整数論的方法の有効性について述べてみたい。A を閉体上のアーベ

ル多様体とする。 A' を A と isogeny なアーベル多様体とする。
 さて、 $\text{End}(A) = \text{End}(A) \otimes \mathbb{Q}$ とすると、 $\text{End}^0(A)$ は有限次元
 の半単純環であり、 $\text{End}(A)$ はその整数環である。今 $\text{End}(A)$
 が極大整数環でかつ類数が1とすると次のことがなりたつ。

A から A' への isogeny φ 对、 $\varphi^{-1} \text{End}(A') \varphi \subset \text{End}(A)$
 なるものが存在する。

つまり、 isogeny を上手に選べば、 $\text{End}(A')$ はその isogeny
 を通じて皆 $\text{End}(A)$ にもちあがる。証明は非常に簡単で、次
 の通りである。 $\text{Hom}(A, A')$ は右 $\text{End}(A)$ -加群であり、

$\text{End}(A)$ の類数1より、 $\text{Hom}(A, A') = \varphi \text{End}(A)$ なる φ があ
 る。 $\lambda \in \text{End}(A')$ なら $\lambda \varphi \in \varphi \text{End}(A)$ となる。//

たとえば、 E が supersingular elliptic curve の時、

$A = E^n$ とおくと、 $n \geq 2$ なら上の仮定はみたされている。

(類数が1であることは、強近似定理による。) また $n=2$
 なら、 $A' \sim E^2$ (isogeny) なる A' について、 $\text{End}(A')$ を具体的に
 書くことが出来る。(cf. [1]) これらを代数幾何のみ
 を用いて示すのはむづかしいのではないかと思う。

§2. Supersingular elliptic curve

この節では、 supersingular elliptic curve について、
 古典的に知られている結果について述べる。内容を、後の拡張
 のことを考えて箇条書きにする。結果は Deuring, Eichler

等による。

以下、 E を標数 $p > 0$ の閉体上の supersingular elliptic curve をあらわし、 $\text{End}(E)$, $\text{Aut}(E)$ を群多様体として、準同型環及び自己同型群をあらわす。

(1) $\text{End}^0(E) = \text{End}(E) \otimes \mathbb{Q} = B$ とおくと、 B は p と ∞ でちょうど分岐する定符号 4 元数環であり、 $\text{End}(E) = \mathcal{O}$ とおくと \mathcal{O} は B の極大整数環である。

(2) 閉体上の supersingular elliptic curves の同型類は、 B の類数 H と個数が等しい。また (当然であるが) E の主偏極は唯一つである。

(3) $\text{Aut}(E) \cong \mathbb{Z}/2$ or $\mathbb{Z}/4$ or $\mathbb{Z}/6$ である。

(4) E は皆 \mathbb{F}_p^2 上の model を持つ。また、 \mathbb{F}_p 上の model を持つものの閉体上の同型類の個数は、 $2T - H$ である。但しここで H は B の類数、 T は B の type number, すなわち B 内の極大整数環の同型類の個数である。

(5) \mathbb{F}_p^2 上の supersingular elliptic curve で、 \mathbb{F}_p^2 -有理点の個数が、 $1 + p^2 + 2p$ 及び $1 + p^2 - 2p$ のものがある。それぞれ存在する。(この個数は Weil の評価式の最大及び最小である。)

以上で H 及び T の値はよく知られているが省略する。

§3. 一般化の準備

前節の内容は、その一部は完全に一般次元に拡張され、またその一部は部分的拡張がなされている。そのために必要な数論的概念について説明したい。前節の4元数環 B にかゝる数論的不変量は、実際には代数群 B^\times の概念であり、 B^\times は \mathbb{Q} で考えれば $GL_2(\mathbb{C})$ である。これは (semi-simple part をとれば) A_1 型でもあり C_1 型でもある。よってこの一般化としては、たとえば $GL_n(B) = M_n(B)^\times$ 及び、quaternion hermitian group G_n :

$$G_n = \{ g \in M_n(B) \ ; \ g^t \bar{g} = n(g) 1_n \}$$

$$n(g) \in \mathbb{Q}^\times$$

の2つが考えられる。ところで $M_n(B)$ の類数は $n \geq 2$ なら1であり、(強近似定理) この事実、 n 個 ($n \geq 2$) の supersingular elliptic curves の直積は、curves をどう選んでも同型という Deligne-Ogus-Serre-Shioda の定理に、反映されている。これ以外の部分では、 G_n の方が中心的役割を果たす。さて、とりあえず、類数と type number について説明したい。

B^n 内の lattice L を考える。 B の極大整数環 \mathcal{O} を1つ固定する。 L が left \mathcal{O} -module であるとき、 L を \mathcal{O} -lattice と呼ぶ。さて、次のような left \mathcal{O} -lattices の集合 $\mathcal{L}(L)$

を考えよう。

$$\begin{aligned} \mathcal{L}(L) &= \{ M \subset B^n; M \text{ は left } \mathcal{O}\text{-lattice } \mathbb{Z}^n \text{ の素数 } v \\ &\text{ に対し } M \otimes \mathbb{Z}_v = (L \otimes \mathbb{Z}_v) g_v \\ &\text{ for some } g_v \in G_v \} \end{aligned}$$

ここで \mathbb{Z}_v は v 進整数環, G_v は G_n の p -アデール化の v -part すなわち,

$$G_v = \{ g \in GL_n(B \otimes \mathbb{Q}_v); g^t \bar{g} = h(g) 1_n, h(g) \in \mathbb{Q}_v^\times \}$$

である。 \mathbb{Q}_v は v 進数体である。(標数の p と区別したいので v と書いた。) 上のような集合 $\mathcal{L}(L)$ のことを、 L に属する種 (genus) という。このうち、極大 \mathcal{O} -lattice と呼ばれる lattices の集合は 2 つの genus にわかれることが知られている。(Shimura による) 1 つは \mathcal{O}^n を含む種 $\mathcal{L}(\mathcal{O}^n)$ であり,

principal genus と呼ばれる。他の 1 つは、これと区別するため、non principal genus と呼ぶ。両者共幾何学的意味を持つ。さて一般の $\mathcal{L}(L)$ に戻そう。 $\mathcal{L}(L)$ にはあきらかに右から G が作用しているが、この G -orbit は有限個しかない。これを $\mathcal{L}(L)$ の類数という。

$$\mathcal{L}(L) \text{ の類数} = \# (\mathcal{L}(L)/G_n)$$

この量は、勿論 $\mathcal{L}(L)$ のとり方にはよってゐる。但し、

principal genus 及び non principal genus の類数は、極大整数環 \mathcal{O} の選び方にはよらない。

次に B の type number の拡張を考える。 B の type number は B の 極大整数環の同型類の個数のことであつたが、Skolem-Noether の定理より、極大整数環の B^* -共役類の個数といふことも同じことである。我々は B^* の拡張として G_n を考えているのであるから、一般化は次のように定義すればよい。

$L(\mathcal{O}^n)/G_n$ の代表系を L_1, \dots, L_H とする。 $M_n(B)$ の部分環 R_i を各 $i=1 \sim H$ に対し、

$$R_i = \{g \in M_n(B) ; L_i g \subset L_i\}$$

と定義する。 (R_i は実は皆極大整数環であり、 $n \geq 2$ なら、皆 $M_n(\mathcal{O})$ と同型になる。) R_i と R_j は、ある G_n の元 g に対し $g^{-1} R_i g = R_j$ となるとき G_n -共役という。

$\{R_1, \dots, R_H\}$ の G_n -共役類の個数を G_n の type number と呼ぶ。

$$G_n \text{ の type number} = \# (\{R_1, \dots, R_H\} / \sim_{G_n\text{-共役}})$$

もう一つだけ記号を準備しておく。任意の \mathcal{O} -lattice L に対し、 L の metric を変えない自己同型のなす群を $\text{Aut}(L)$ とかく。すなわち

$$\text{Aut}(L) = \{g \in G_n ; Lg = L\}$$

なお、以上の諸概念は、アデールを用いた方が説明がすっきりするが、当研究集会の性格を考慮に入れ、敢えてアデールなしで済ませた。

§4. Supersingular abelian varieties

E を supersingular elliptic curve, n を $n \geq 2$ なる自然数とする。 n 次元アーベル多様体 A は $A \cong E^n$ のとき

superspecial, $A \sim E^n$ (isogeny) のとき supersingular という。この節の目的は §2 の内容が上のような A について、どの程度拡張されているかを述べることにある。あえて定理とは書かず、§2 の番号にあわせて、順に箇条書きにしてみたい。moduli に関することはあとで述べる。

(1) A が supersingular ならば勿論 $\text{End}^0(A) \cong M_n(B)$ である。しかし $\text{End}(A)$ は一般には極大整数環ではない。たとえば、 $n=2$ なら極大整数環以外に2種類あらわれる。(手法は §1 に述べた通り。) $n \geq 3$ は知られていない。

(2) 主偏極 superspecial abelian variety (E^n, Θ) の同型類の個数は、 $\mathcal{L}(\mathcal{O}^n)$ の類数 H に等しい。(cf. [11])

(3) (E^n, Θ) と上の (2) で自然に対応する $L \in \mathcal{L}(\mathcal{O}^n)$ に対し主偏極アーベル多様体としての自己同型群を $\text{Aut}(E^n, \Theta)$ と書くと

$$\text{Aut}(E^n, \Theta) \cong \text{Aut}(L) \quad \text{である。また、}$$

$n=2$ ならば $\text{Aut}(E^2, \Theta)$ は皆具体的にわかる。(cf. [1])

(4) E とし \mathbb{F}_{p^2} 上定義されたものを取、この場合、主偏極アーベル多様体 (E^n, Θ) はいつでも \mathbb{F}_{p^2} -rational である。また、 (E^n, Θ) のうち \mathbb{F}_p 上定義された model (A, C)

を持つもの、閉体上の同型類の個数は $2T-H$ である。但しここ 2 は G_n の type number である。(cf. [2])

(5) $p \neq 2$ ならば、 \mathbb{F}_p 上で定義された genus 3 の curve である \mathbb{F}_p -有理点の個数が $1+p^2+6p$ のものが存在する。

(cf. [3]) これは Weil の評価式の最大値である。(genus 2 の curve は Serre の結果がある。)

さて、 $n \geq 2$ の時と $n=1$ の時の 1 つの違いは、 $n \geq 2$ の時には、moduli の次元があることである。主偏極アーベル多様体の moduli を $A_{n,1}$ とするとき、supersingular abelian varieties のなす $A_{n,1}$ 内の locus は、一般に既約ではない。既約成分の個数については既に桂氏も書いているので、ここではくり返さないが、少し他の面について述べてみたい。今 $n=2$ とすると上記の locus の既約成分の個数は、non principal genus の類数に等しく、また各既約成分の normalization は \mathbb{P}^1 に等しいことが知られている。(Katsura-Oort) とのこと。その各成分には superspecial なものがある。つまり、こちらは principal genus の類数個あるのであるから、全体の各成分にとりよりの、ているのが気になるところである。実はこれが数論的な判定条件に与るばかりではなく、も、と面白いこともわかる。これらを説明するには今少し数論的概念に深入りせねばならない。

今、 $n=2$ とし、 $\mathcal{L}, \mathcal{L}'$ を B^2 の principal 及び non-principal genus とする。 $L \in \mathcal{L}, L' \in \mathcal{L}'$ とし、すべし素数 v に対し

$$U_v = \{g \in G_v; (L \otimes \mathbb{Z}_v)g = L \otimes \mathbb{Z}_v\}$$

$$U'_v = \{g \in G_v; (L' \otimes \mathbb{Z}_v)g = L' \otimes \mathbb{Z}_v\}$$

とおく。 G_A を G_2 の adèle 化とする。 G_A の部分群 U, U' を、 G_∞ を G_A の ∞ 成分として

$$U = G_\infty \cdot \prod_v U_v, \quad U' = G_\infty \cdot \prod_v U'_v$$

とおく。 G_A をそれぞれについて次のように double coset に分解する。

$$G_A = \bigsqcup_{i=1}^H U g_i G, \quad G'_A = \bigsqcup_{i=1}^{H'} U'_i g'_i G$$

ここで H, H' はそれぞれ $\mathcal{L}, \mathcal{L}'$ の類数である。 L, L' をうまく選べば、 $v \neq p$ については $U_v = U'_v$, $v = p$ については $U_p \cap U'_p$ が G_p の minimal parahoric 群となるようにしておける。これを仮定し、 $U_0 = G_\infty \cdot \prod_{v \neq p} U_v \cdot (U_p \cap U'_p)$ とおく。また

$$G_A = \bigsqcup_{i=1}^{H_0} U_0 g_i'' G$$

とする。(H_0 は U_0 の類数ともいうべき量だが、この場合は対応する lattice があるわけではない。) さて、 $U g_i G$ と $U'_i g'_i G$ の間には何の包含関係もないが、 $U_0 g_i'' G$ は、どこか $U-G$ -double coset 及び $U'-G$ -double coset に属するわけである。

定理 (1) $U'_g: G$ に対応する既約成分に. $U_g: G$ に対応する主偏極アーベル多様体 (E^2, Θ) が, 2 であるための必要十分条件は. $U'_g: G$, $U_g: G$ が共に共通の $U_0: g: G$ を 1 つは含むことである。

(2) 2 次元主偏極 supersingular abelian surfaces の locus の arithmetic genus $= H_0 - H_1 - H_2 + 1$ である。

ここ 2 $H_0 - H_1 - H_2 + 1$ という量は. U_0 に属する, weight 0 の保型形式のうち 2 new forms の次元であり, Jacquet-Langlands 対応の拡張を考へる際に重要であった。
(cf. [4])

なお, 以上のような考察は, locus の連結性を示すためにも有効である $n=2$ では, 上と Bruhat-Tits theory 及び強近似定理で連結性が示せる。(Ekedahl) $n=3$ では locus の連結性は, ある種の Hecke operator の決める Brandt 行列の連結性と強近似定理に帰着する。(連結性は Ekedahl-Oort も得ているようであるが, 私の証明とどういう関係がよく知らない。) なお, 一般次元の locus のより深い構造については, まだ知られていない。この部分は最終的には G_n の数論により統制されるはずだと考えている。locus は smooth ではないので arith. genus 等のことはよくわからない。($n=2$ 2

は、たまたま locus が 1 次元な g^2 、特異点がある、 g^2 も、arithmetic genus が定義される。))

もう一つ述べる。level 2 の moduli $A_{2,1,2}$ から $A_{2,1}$ への covering を考へる。ここ g^2 locus の covering を考へると、実は各 $L \in \mathcal{L}'/G_2$ に対し、 $\text{Aut}(L)$ は、対応する既約成分の分解群になる、という。また、具体的にすべて求めることもできる。(cf. [5])

§5. 手法上の注意

§4 で述べたことをどのようにして証明するか、数論上のポイントに限って述べてみたい。数論上の手がかりは、 G_n や lattice, Hecke operator 等にしかない g^2 あるから、幾何学を全部これらの言葉に翻訳する必要がある。たとえば、Néron-Severi 群を $\text{End}(A)$ の一部と同一視することにし、すべてをなるべく algebra または群論で考へるわけである。たとえば、定義体に関することであれば、Frobenius 写像が問題になるが、これを algebra の元と思つて、Weil criterion などを G_n の特殊な元の存在条件のようなものにおきかえる。その後は、跡公式等の手法で、具体的な計算を実行するわけである。実際には、このような過程で実は数論的手段も不足していることがわかり、新しく理論を作った部分もある。

たとえば、1つの種 L に対し、 $L/G = \{L_1, \dots, L_H\}$ とする
とき、 $\text{Aut}(L_i)$ を一斉に与える方法が知られていないが、た。
これを原理的に解決し、また $n=2$ の場合に計算してみせた
のが [57] である。このあたりは、今の代数幾何的な手法で
は無理のように見える。また、十分多くの \mathbb{F}_p 有理点を持つ、

genus 3 の curve の存在証明も、ある種の mass が正になる 2
とを用いていて、存在定理であり、代数幾何的に構成するわけ
ではない。

supersingular abelian varieties の理論では、まだまだ、
数論が full に使われているとは言えない面もあり、今後を
発展してゆくと思われる。

文献 (拙稿の項も参照された)。)

- [1] T. Ibukiyama, T. Katsura, and F. Oort, Supersingular
curves of genus two and class numbers, *Compositio Math.*
57 (1986)
- [2] T. Ibukiyama and T. Katsura, On the field of definition
of supersingular polarized abelian varieties and type numbers,
preprint
- [3] T. Ibukiyama, On rational points of curves of genus
three over finite fields, preprint

- [4] K. Hashimoto and T. Ibukiyama, On relations of dimensions of automorphic forms of $Sp(2, \mathbb{R})$ and its compact twist $Sp(2)$ (II) Adv. Stud. Pure Math. 7, 1985, 30-102
- [5] T. Ibukiyama, On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula, Adv. Stud. Pure Math. 15, 1989, 301-349